Computer Emergency Response Team

Porto, 19th September 2007

EUROPOL

Structure of the presentation

- What is Europol ?
- Europol as Intelligence Tool:

  Analytical Work File (AWF)
- High Tech Crimes:

  The Perspective of Europol

What Europol is

- EUROPOL is European Police Office that handle intelligence through the information exchange and analysis of information between and with the Member States

- EUROPOL has the aim to improve the effectiveness and the cooperation amongst the competent Member States' authorities in the prevention and repression of *organized crime* which has trans-national dimensions

- EUROPOL operating within its mandate is an intelligence service that has as target the *criminal organizations*

- EUROPOL is embedded in the 3rd pillar

What Europol is not

EUROPOL is not: European Branch of Interpol

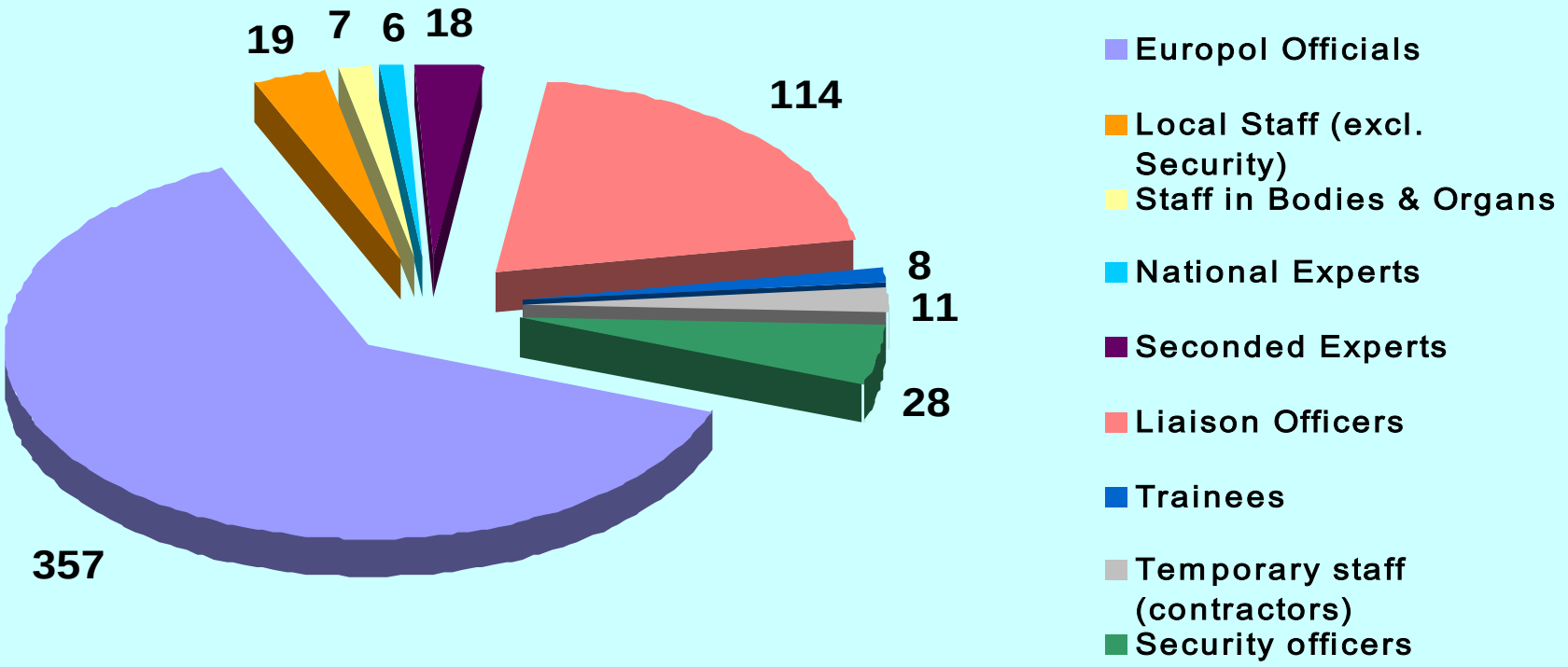
EUROPOL is not: European FBI

EUROPOL is not: A Supranational Organism

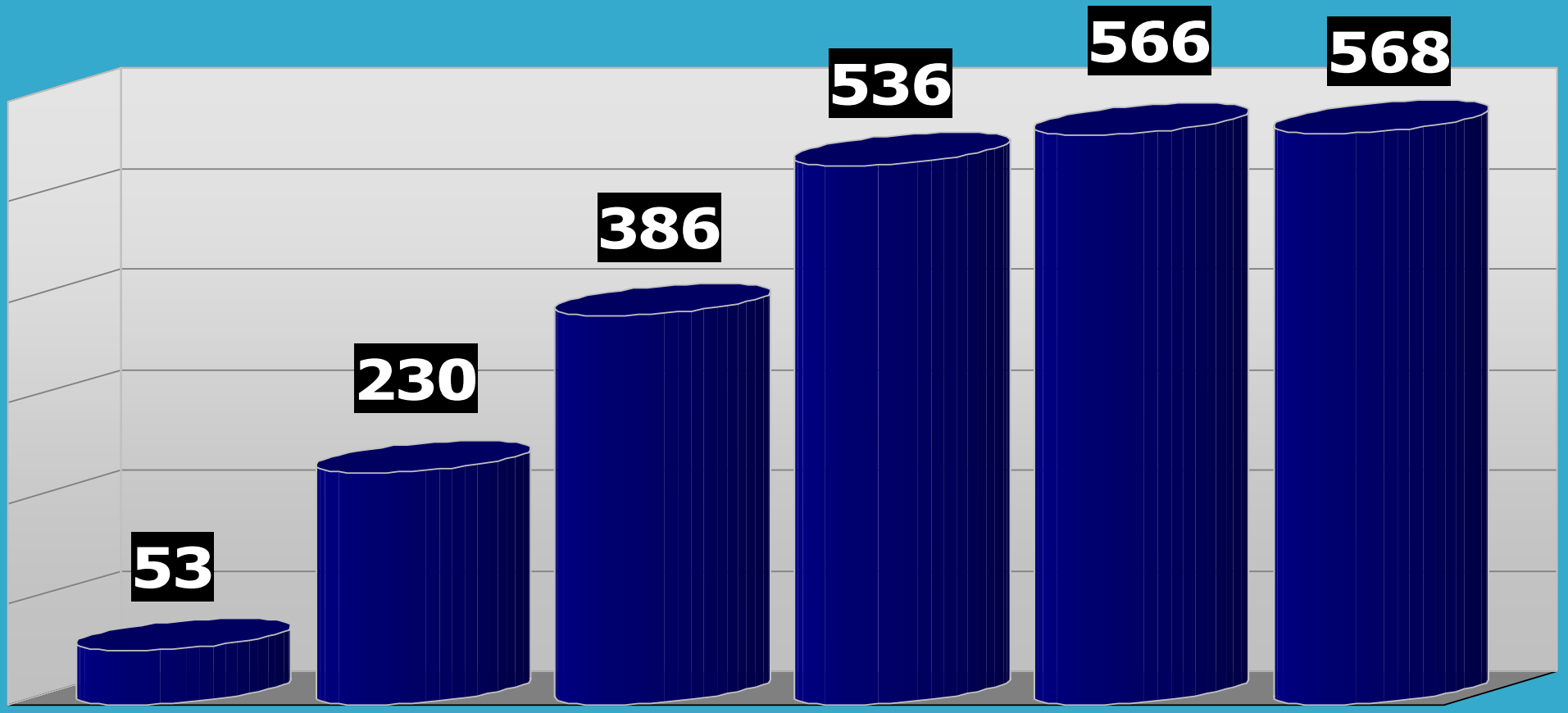
Why Europol

- Borders' issues
- Different legal and procedural systems
- Different roles & responsibilities of Police Forces
- Different roles & Responsibilities of Judicial Authorities
- Limitations in coordination and information analysis
- Linguistic Barriers

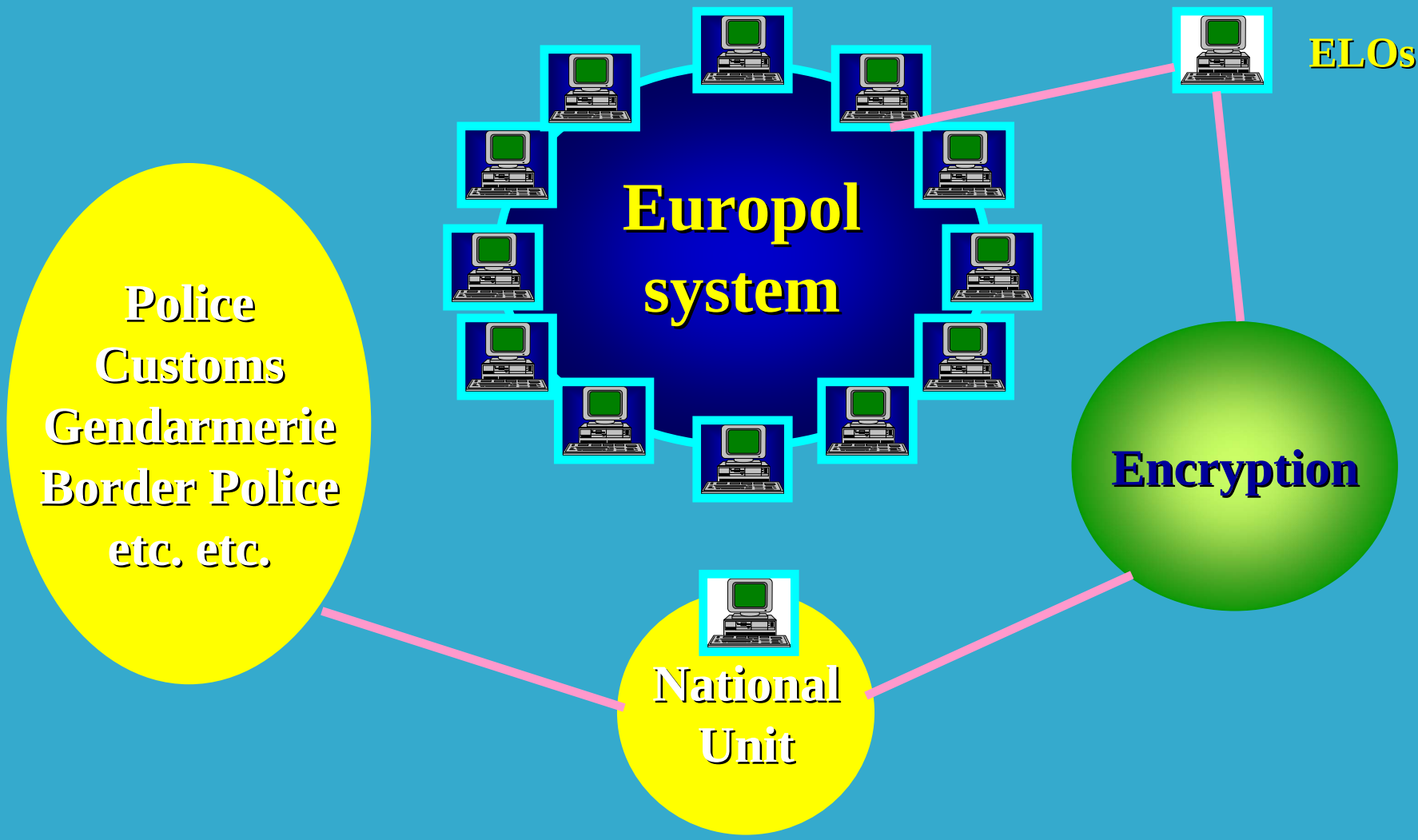
Europol Personnel in August 2007

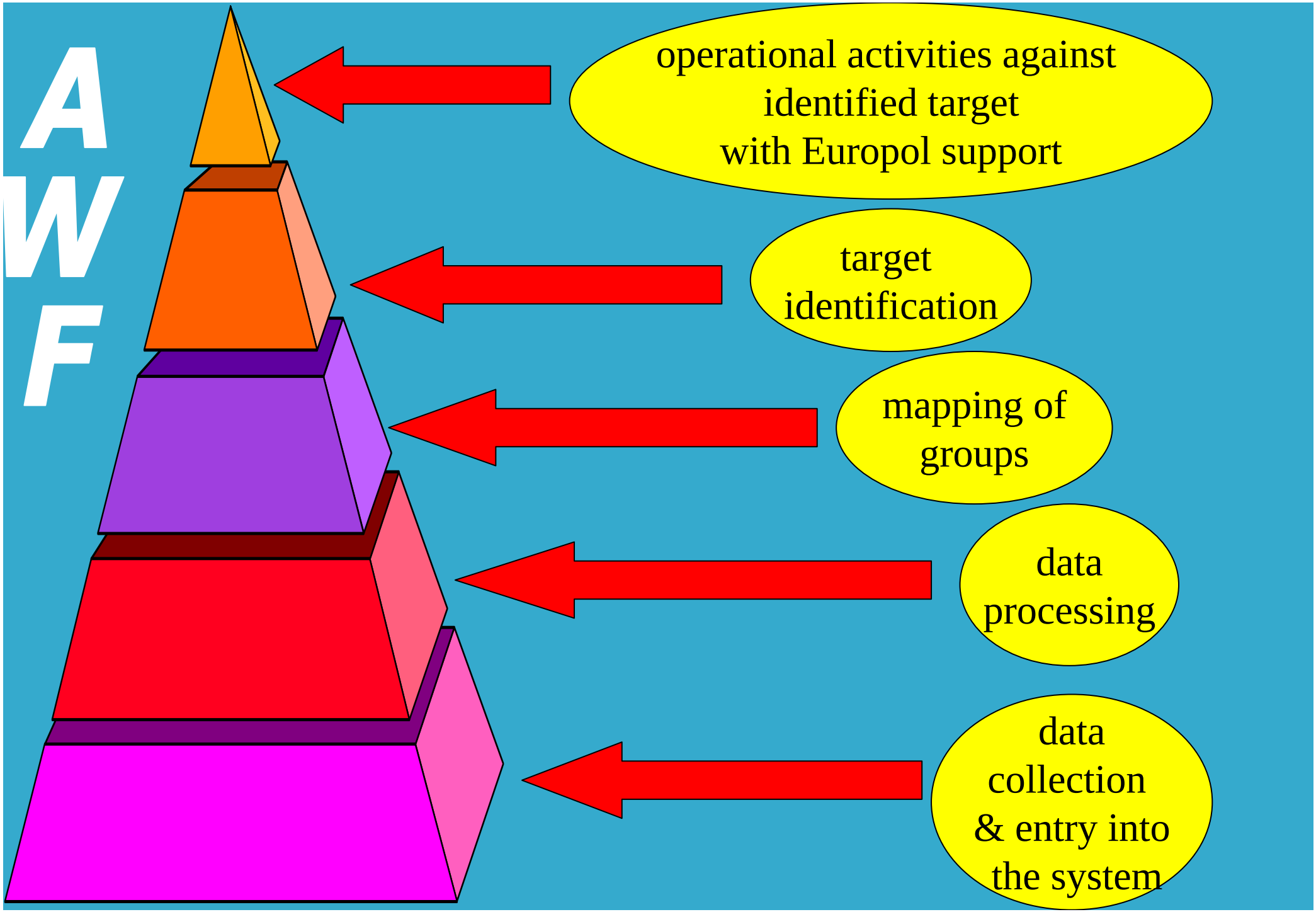


Personnel of Europol



Europol system




AWF
operational activities against identified target with Europol support
target identification
mapping of groups
data processing
data collection & entry into the system

High Tech Crime Centre at Europol

4 Officials:

- 1 First Officer Team Leader
- 1 First Officer
- 2 Second Officers

Embedded in the Serious Crimes Department

Role, tasks and responsibilities

To maintain a high level of expertise in High Tech Crimes through coordination, training and operational support

How?

- Organising Expert Meetings
- Reinforcing the Networking with HTCUs
- Participation at International Working Groups
- Participation at International Conferences
- Strengthening the Relationship with Private Sector and Academic World
- Drafting Threat Assessments on HTC
- Investing in Training Courses
- Providing Operational Support

High Tech Crimes

CYBER CRIME: **computer as TARGET**

- **Hacking (D-DOS, Botnets, Zombies…)**
- **Malwares (Virus, Worms, Trojans…)**
- **Spamming (blackmail, cyber-stalking…)**

COMPUTER RELATED CRIME: **computer as TOOL**

E-Frauds, E-Laundering, Child Pornography, E-Terrorism, Phishing, ID-Theft, Drugs, Extortions….

EUROPOL

The Usage of Internet

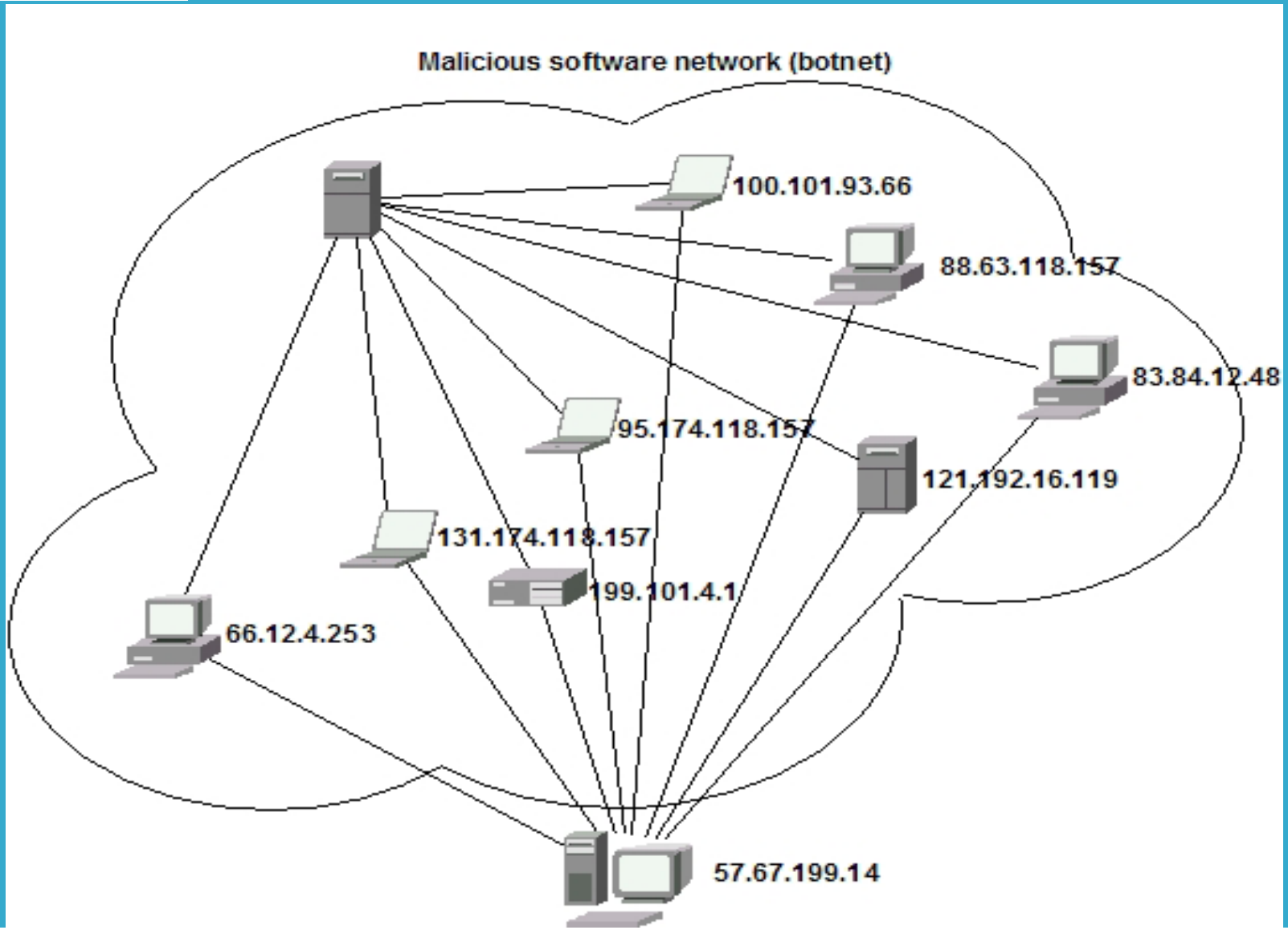
http://www.internetworldstats.com/stats.htm

WORLD INTERNET USAGE AND POPULATION STATISTICS

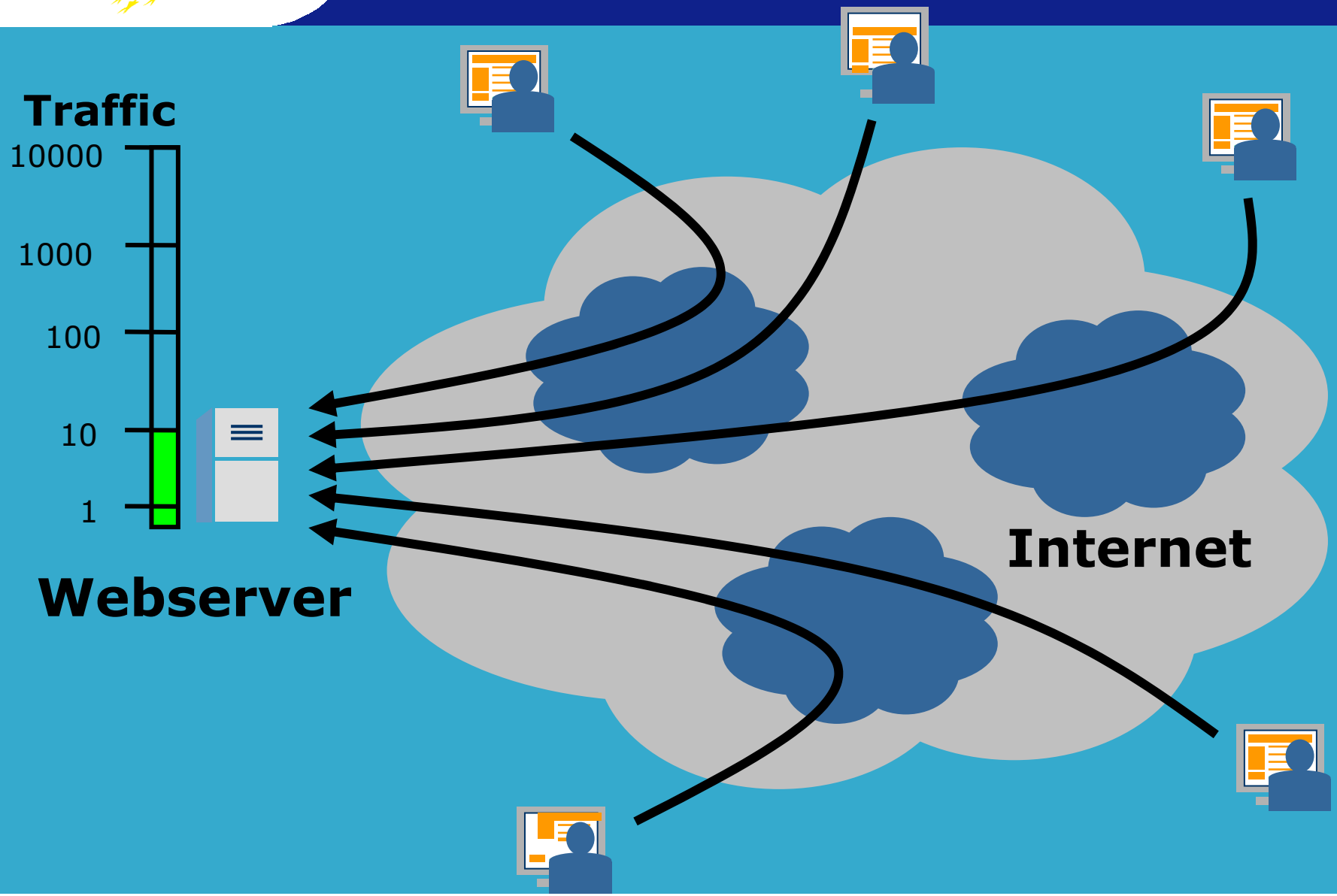
World Regions	Population (2007 Est.)	Population % of World	Internet Usage, Latest Data	% Population (Penetration)	Usage % of World	Usage Growth 2000-2007
Africa	933,448,292	14.2 %	**33,545,600**	3.6 %	2.9 %	643.1 %
Asia	3,712,527,624	56.5 %	**436,758,162**	11.8 %	37.2 %	282.1 %
Europe	809,624,686	12.3 %	**321,853,477**	39.8 %	27.4%	206.2 %
Middle East	193,452,727	2.9 %	**19,539,300**	10.1 %	1.7 %	494.8 %
North America	334,538,018	5.1 %	**232,655,287**	69.5 %	19.8%	115.2 %
Latin America/Caribbean	556,606,627	8.5 %	**109,961,609**	19.8 %	9.4 %	508.6 %
Oceania / Australia	34,468,443	0.5 %	**18,796,490**	54.5 %	1.6 %	146.7 %
WORLD TOTAL	6,574,666,417	100.0 %	**1,173,109,925**	17.8 %	100.0 %	225.0 %

NOTES: (1) Internet Usage and World Population Statistics are final for **June 30, 2007**. (2) CLICK on each world region for detailed regional information. (3) Demographic (Population) numbers are based on data contained in the world-gazetteer website. (4) Internet usage information comes from data published by Nielsen//NetRatings, by the International Telecommunications Union, by local NICs, and other other reliable sources. (5) For definitions, disclaimer, and navigation help, see the Site Surfing Guide. (6) Information from this site may be cited, giving due credit and establishing an active link back to www.internetworldstats.com.

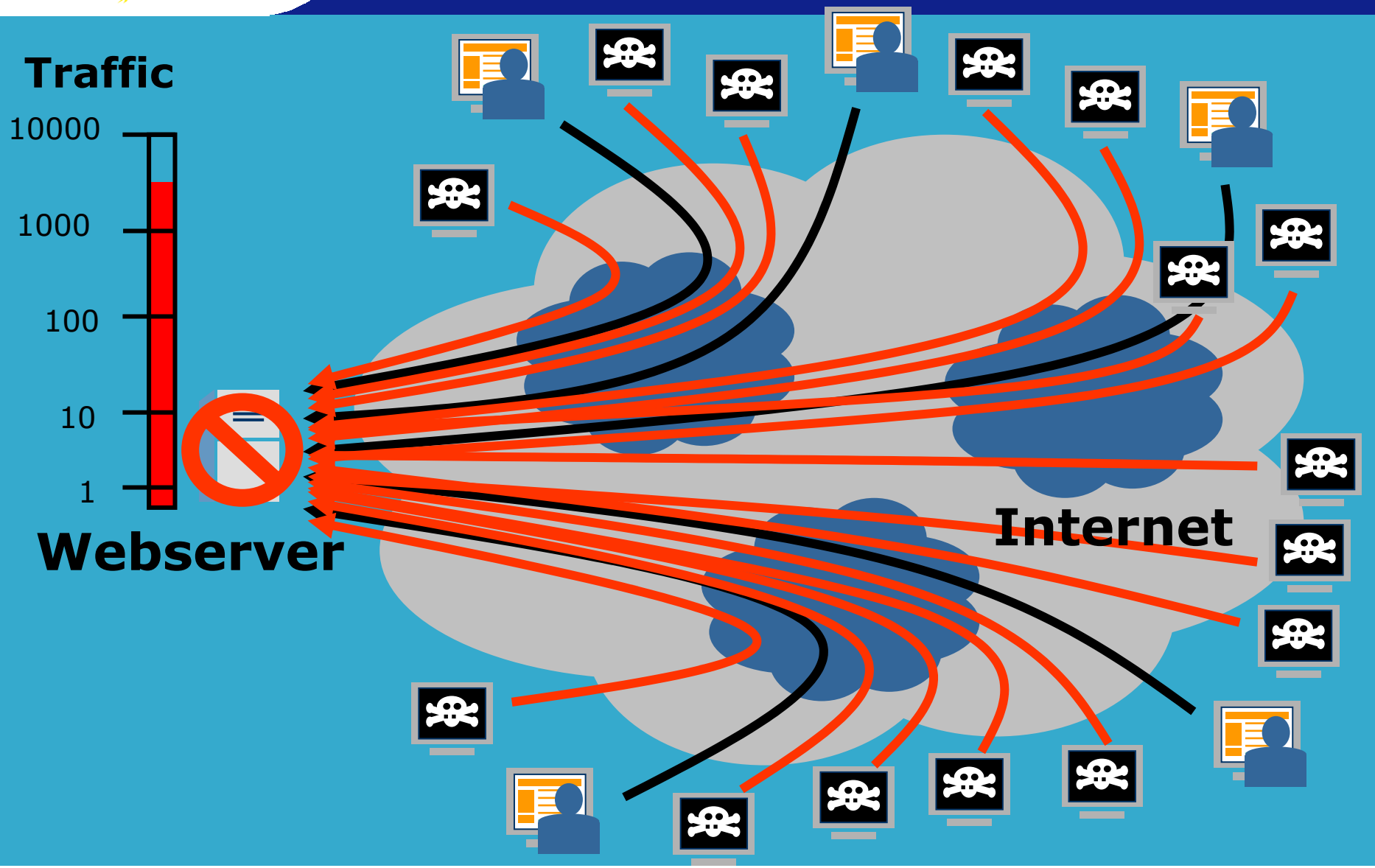
Crime Types: BOTNETS and Crimewares



Crime Types: BOTNETS and Crimewares



Crime Types: BOTNETS and Crimewares



BOTNETS and Crimewares

- Hackers remotely manipulate millions of compromised machines
- BOTNETS come in many varieties, providing an avenue to spread new crimewares and earn money (extortions)
- New generation of crimewares points at extracting data
- Hackers are well organised and split their activities between compromising machines.
- It is very difficult to work on prevention
- ISP are not always efficient
- There are several initiatives at an international level

Critical Information Infrastructures (CII)

What is critical? A definition?

Physical and IT facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on health, safety, security or economic well-being of citizens or effective functioning of governments.

European Commission - DGTREN – Security Directorate

Attack to Critical Information Infrastructures (CII)

- Convergence is the main issue to manage
- CII become targets of attacks
- Critical information needs to be protected
- Systems are interconnected but lack of interoperability
- Several initiatives at EU level and overseas
- Still little coordination and common strategy at EU level
- Difficulties in incident response
- Difficulties in making a risk assessment

Social Engineering over Internet: Phishing and Its Varieties

- **Phishing**: a combination of E-Fraud and Identity Theft
  - It causes enormous financial losses in terms of lack of revenue and customers' lack of trust in legitimate products
  - There are several initiatives worldwide to combat phishing
  - Organised Crime uses these new e-crime facilities
  - The money obtained by phishing is laundered through other e-facilities

- **Pharming:** Manipulation of Domain Name Server
- **Vishing:** A new trend for criminals to phish over IP
- **SMiShing:** A new trend for criminals to phish over Mobile Phones SMS

Cyber Terrorism

- Terrorist organisations have understood how to use technology for their purposes
- There are real cyber terrorists and black hats hired to serve terrorist organisations
- Exploit technology for propaganda, spread of fear, enhance communication amongst inners, and perpetrate attack against enemies' targets
- Internet is also used to e-train members of criminal organisations
- Critical Information Infrastructures networks are also targets

Trafficking of Child Pornography Images on the Internet

- Child abusers and Child pornographers
- The phenomenon of child pornography is continuously growing
- New technology such as WI-FI, VoIP and Pay-per-View
- Peer to Peer most used for exchange of pictures
- CP generates huge revenues
- More control needed toward the children by families, social entities, governments

Drugs trafficking over Internet

- There is widespread use of internet pharmacies without proper control
- Web sites and forums on the internet
- Trade in precursors to produce synthetic drugs.
- There is an increase of clandestine laboratories that sell drugs using the internet.
- There is a need for more consistent cooperation between law enforcement and private industry in order to better detect the illicit traffic of drugs over the internet.

Cyber Criminals' Communities

- Depicting the structure of these groups and their interactions is very difficult for many reasons, some of them can be:
  - the communities have still young life
  - there is little background about them
  - little information is still written.

- Cyber criminals' may be driven by several motives (ideology, status, self–esteem, money)
- Groups of criminals operating on the internet are usually heterogeneous
- The heterogeneity is determined by the driven factors such as MONEY
- The homogeneity is instead mainly driven by ideals

Organized Crime

- Organised Crime is difficult to map out because Internet has not boundaries; information is too spread and the collection of data is difficult
- Organised crime use horizontally High Technology to pursue criminal goals
- Many individuals have links with criminal organisations
- There is still a huge lack of data about organised crime on the internet
- High Tech make the structure of criminal groups very flexible

The future??

- New approach on use of internet, growth of on line groups
- A lot of services online
- Large storage of data to remote servers offered
- Managing services from remote…going back to mainframe concepts?....
- Going more for VOIP
- More encrypted applications (e.g. Instant Messaging)

Conclusions

- The horizontal use of hi-tech is more and more beneficial for criminals
- There is a rapid growth of underground economy through attacking computer systems: driving factor for criminals is usually money.
- HTC is beginning to be of public concern to the public: threat to critical information infrastructure networks

Conclusions

- Consistent growth of social engineering on the internet: the Identity Theft is strongly involved as well as the theft of financial data
- Increase of child abusive content distributed and exchanged on internet
- The main critical issues are still users' authentication, anonymity and encryption

A Desirable Action

- Education of internet user in how to utilize technologies
- Creation of common reporting system
- Improvement of a common strategy to protect Critical Information Infrastructures
- Improving the common understanding with the internet stakeholders: private industry, researchers, internet communities
- Large ratification of the Cyber Crime Convention for a common legal platform amongst countries
- Regulation of the public internet accesses (cyber cafés, libraries, university..)

Thank You
for Your Attention

Nicola DILEONE

High Tech Crime Centre

Raamweg 47

PO-Box 90850

2596HN The Hague

The Netherlands

Tel: +31 (0)70 302 51 32

Mob: +31 (0)6 24 82 31 76

Fax: +31 (0)70 318 08 39

Nicola.Dileone@europol.europa.eu

HTCC@europol.europa.eu